

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JOHN KANE;
ANDRE NESTOR.

Defendants.

2:11-cr-00022-JCM-RJJ

REPORT & RECOMMENDATION
OF UNITED STATES
MAGISTRATE JUDGE

(Motion to Dismiss (#56)
Motion to Dismiss (#57) &
Motion for Joinder (#62))

This matter is before the Court on Defendant John Kane's Motion to Dismiss (#56); Defendant Andre Nestor's Motion to Dismiss (#56); and Defendants John Kane's Motion for Joinder to Defendant Andre Nestor's Motion to Dismiss (#62). The Court has also reviewed the Government's Response (#68) and Defendants' Replies (#71) and (#78), respectively.

BACKGROUND

On January 19, 2011, the Government filed the Indictment (#12) in this case. The Government alleges that from about April 2009 to September 2009 Kane and Nestor devised a way to exploit video poker machines, winning several hundred thousand dollars.

Video poker machines offer different varieties of poker for customers to play. To exploit the video gaming machines, the Government alleges that the Defendants would ask a casino employee to activate the "double up" feature on certain video poker machines. Essentially, the "double up" feature allows casino patrons to double their winnings or lose their bet. The Defendants then legitimately played video poker until they obtained a winning hand of cards and collected their proper winnings. The Government alleges that the Defendants then used a

1 complex combination of game changes, bill insertions and cash outs to access previous winning
2 hands of cards, use the “double up” feature to change the denomination in the middle of the game
3 to the highest denomination, and trigger a second jackpot. Because of a series of programming
4 errors, the machine re-evaluated the original game at the new, higher denomination, triggering a
5 jackpot which paid out at a higher denomination than the Defendants had initially wagered. The
6 Government does not allege that the Defendants physically tampered with the video poker
7 machines in any way.

8 The Defendants filed the present Motions to Dismiss (#56) (#57) moving the Court to
9 dismiss Counts 2 and 3 of the Indictment (#12), alleging computer fraud. The Defendants are
10 charged with violating certain provisions of the Computer Fraud and Abuse Act (CFAA).
11 Specifically, the Government alleges that the Defendants “did knowingly and with intent to
12 defraud access a protected computer exceeding his authorized access and by means of such
13 conduct furthered the intended fraud and obtained something of value, specifically, money, all in
14 violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A).” Indictment (#12) at
15 3-4.

16 With a few exceptions which will be discussed further, Kane and Nestor raise the same
17 main arguments in each of the Motions to Dismiss. For purposes of these Motions (#56) (#57),
18 the Defendants argue that, even accepting all of the Government’s factual allegations as true, the
19 Government has failed to state a cognizable offense under the law. The Defendants assert that
20 they have not violated the CFAA because: (1) a video poker machine is not a “protected
21 computer” under the statute; and (2) the Defendants’ actions did not “exceed [their] authorized
22 access” to the video poker machines.¹

23 ///

24 ///

25
26 ¹ Although these arguments are common between the motions to dismiss, each defendant asserts at
27 least one argument that is not echoed in his co-defendant’s motion to dismiss. In his Reply (#71), Kane
28 asserts that video poker machines are not even “computers,” much less “protected computers” under the
CFAA. Nestor raises two unique arguments of his own. First, Nestor argues that he did not “access” the video
poker machines, as that term is understood under the CFAA. Second, Nestor argues that 18 U.S.C. §
1030(a)(4) is unconstitutionally vague. Kane adopts these arguments in his Motion for Joinder (#62).

DISCUSSION

A motion to dismiss for failure to state an offense is governed by Rule 12(b) of the Federal Rules of Criminal Procedure. Rule 12(b)(3)(B) allows the Court to hear a claim that “the indictment or information fails to invoke the court’s jurisdiction or to state an offense.” In the much cited *United States v. Boren*, 278 F.3d 911 (9th Cir. 2002), the Ninth Circuit addressed the correct analysis of such a motion.

In ruling on a pre-trial motion to dismiss an indictment for failure to state an offense, the district court is bound by the four corners of the indictment. On a motion to dismiss an indictment for failure to state an offense, the court must accept the truth of the allegations in the indictment in analyzing whether a cognizable offense has been charged. The indictment either states an offense or it doesn’t. There is no reason to conduct an evidentiary hearing.

Boren, 278 F.3d at 914 (internal citations omitted). Thus, in order to withstand the instant Motions to Dismiss (#56) (#57) the indictment must allege that the Defendants performed acts that, if proven, constitute a violation of the law under which they have been charged. *Id.*

An indictment need only be a “plain, concise, and definite written statement of the essential facts constituting the offense charged.” Fed.R.Crim.P. 7(c)(1). For purposes of due process, an indictment is sufficient if it states “the elements of the offense charged with sufficient clarity to apprise a defendant of the charge against him, primarily so that he can defend himself against the charge and plead double jeopardy in appropriate cases.” *United States v. Johnson*, 804 F.2d 1078, 1084 (9th Cir. 1986) (citations omitted).

The Defendants argue that the Indictment (#12) fails because the facts alleged, even when accepted as true, do not amount to a cognizable offense under the statute. Title 18 U.S.C. § 1030(a)(4), the statute under which the Defendants are charged, makes it a crime if anyone:

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

Id. The Defendants assert that they have not violated this statute because: (1) a video poker machine is not a “protected computer” under the statute; and (2) the Defendants’ actions did not “exceed [their] authorized access” to the video poker machines.

1 I. Protected Computer

2 Under 18 U.S.C. § 1030 a “computer” is defined as “an electronic, magnetic, optical,
3 electrochemical, or other high speed data processing device performing logical, arithmetic, or
4 storage functions, and includes any data storage facility or communications facility directly
5 related to or operating in conjunction with such device,” carving out explicit exceptions for “an
6 automated typewriter or typesetter, a portable hand held calculator, or other similar device.” 18
7 U.S.C. § 1030(e)(1). The statute defines a “protected computer” as a computer “which is used in
8 or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B).

9 While Nestor concedes that, because video poker machines “perform complex logical and
10 storage functions,” they are “probably ‘computers’ for the purposes of the CFAA,” Kane’s
11 Motion to Dismiss (#56) does not address the issue. In his Reply (#71), however, Kane explicitly
12 argues that video poker machines are not “computers.” Kane argues that these machines do not
13 have keyboards, are not connected to any sort of network, and cannot read or accept “new
14 information,” but can only calculate what has previously been included in the program. Kane
15 Reply (#71) at 7. However, 18 U.S.C. § 1030(e)(1) does not require any of these attributes to be a
16 “computer.” The statute carves out a specific exception for certain types of devices and Kane
17 argues that the video poker machines should be considered an “other similar device.” However, a
18 video poker machine is not sufficiently similar to an automated typewriter or typesetter, or a
19 portable hand held calculator to support Kane’s interpretation. The Court agrees with Nestor that
20 a video poker machine performs functions that are directly in line with the CFAA’s definition of
21 “computer.”

22 However, both Kane and Nestor agree that video poker machines are not “protected
23 computers” under the statute. Those courts that have addressed whether a specific computer
24 qualifies as a “protected computer” seem to agree that a connection to the internet is sufficient to
25 establish that a computer was used in interstate commerce and is therefore a “protected
26 computer.” See e.g., *Multiven, Inc. v. Cisco Systems, Inc.*, 725 F.Supp.2d 887, 891-92 (N. D. Cal.
27 2010); *U.S. v. Nosal*, 2012 WL 1176119 at *3 (9th Cir. 2012) (“ ‘protected computer’ is defined
28 as a computer affected by or involved in interstate commerce—effectively all computers with

1 Internet access”); *National City Bank, N.A. v. Prime Lending, Inc.*, 2010 WL 2854247 at *4 n.2
2 (E. D. Wash. 2010) (stating that “any computer connected to the internet is a protected
3 computer”). The Defendants argue that the fact that video poker machines do not access the
4 internet tends to indicate that they are not “protected computers.” The Government, on the other
5 hand, asserts that an internet connection is sufficient, but not necessary, to establish a computer
6 as a “protected computer,” citing *U.S. v. Mitra*, 405 F.3d 492 (7th Cir. 2005).

7 In *Mitra*, the defendant had tapped into the emergency radio system used by the city and
8 sent out false signals. The radio system was completely within the state’s borders and the damage
9 had occurred solely within state boundaries. However, the Seventh Circuit reasoned that the radio
10 spectrum used in this computer-based radio system affected interstate commerce because the
11 electromagnetic spectrum, on which the radio operated, was a “channel of interstate commerce”
12 that was securely within the federal regulatory domain. The defendant argued that his
13 interference did not affect any radio system on the other side of a state line. The court answered
14 as follows:

15 [T]he statute does not ask whether the person who caused the damage acted in interstate
16 commerce; it protects computers (and computerized communication systems) used in
17 such commerce, no matter how the harm is inflicted. Once the computer is used in
interstate commerce, Congress has the power to protect it from a local hammer blow, or
from a local data packet that sends it haywire.

18 *Mitra*, 405 F.3d at 496.

19 However *Mitra* is not binding on this Court and the holding in *Mitra* is inapplicable to
20 these facts. Kane, addressing this issue, argues that the Seventh Circuit’s holding in *Mitra* is
21 inapplicable because video poker machines are not subject to federal regulation like the radio
22 spectrum in *Mitra*. Kane Motion (#56) at 6. The Government on the other hand asserts that
23 gaming machines, such as video poker machines, are subject to federal regulation under the
24 Gambling Devices Act of 1962 (15 U.S.C. § 1171-78). This is incorrect. The Gambling Devices
25 Act does not actually regulate the function of these gambling machines. Whereas the radio
26 spectrum in *Mitra* was regulated by the Federal Communications Commission as an actual
27 channel of interstate commerce, the Gambling Devices Act mainly has to do with the shipping
28 and transportation of these devices within the channels of interstate commerce. The gambling

1 machines themselves do not function within those channels as anything more than cargo.

2 Furthermore, while the Court agrees that internet access is not the only way a computer
3 may be deemed a “protected computer” under the CFAA, there is an important factual distinction
4 between the present case and *Mitra*. Unlike the radio system in *Mitra*, a video poker machine is
5 not used to transmit, receive, or otherwise communicate information across state lines. Although
6 the actual effects were only felt within the state, *Mitra*’s device was capable of reaching across
7 state lines. The video poker machines in this case have no such capability.

8 In order to be classified as a “protected computer,” a computer must be used in or affect
9 interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2)(B). The Government
10 argues that video poker machines affect interstate commerce because “[c]ustomers from all over
11 the country travel to Nevada to play Las Vegas’ gaming machines.” Response (#68) at 5. This
12 argument fails for two reasons. First, this supposed effect on interstate commerce only holds up
13 in the aggregate. While it may be true that the entire Las Vegas gambling industry attracts
14 customers from all over the country, the Government cannot show that individual video poker
15 machines have such an effect on interstate commerce. Second, to follow the Government’s
16 interpretation of the term “protected computer” would divorce the function of the device, i.e.
17 logical, arithmetic, or storage functions, from its supposed effects on interstate commerce.
18 Computers connected to the internet are “protected computers” because this part of their
19 designed function allows them to engage in interstate commerce. Likewise, the function of the
20 radio system in *Mitra* was to connect with a federally regulated channel of interstate commerce.
21 While any individual computer connected to the internet, or the *Mitra* radio system, can
22 instantaneously engage in interstate commerce, an individual video poker machine has no such
23 connection to the wider world.

24 The Government has asserted an extremely attenuated connection between the video
25 poker machines and interstate commerce. This would result in an unacceptably broad application
26 of the term “protected computer.” For example, the cash registers in the Forum Shops at Caesar’s
27 Palace could be considered “protected computers” because customers from all over the country
28 travel to shop at Las Vegas’ world famous shopping center. A “protected computer” must have

1 more than a tangential relationship to interstate commerce. Although people may play gaming
2 machines when they travel to Las Vegas, their use of the machines is incidental to their travels.

3 III. Access

4 Defendant Nestor briefly argues that his motion to dismiss should be granted because he
5 did not actually “access” the video poker machines. Nestor Motion (#57) at 9-10. The CFAA
6 does not define “access” and very few courts have actually discussed the meaning of the term.
7 The cases that have discussed the meaning of “access” dealt with convoluted factual situations
8 where the defendants had allegedly “accessed” computers through some sort of external and
9 extended means. This makes the question of “access” more difficult to answer. For example, the
10 defendant in *State v. Allen*, 917 P.2d 848 (Kan. 1996), used a computerized telephone device to
11 repeatedly call the telephone company computer that controlled long-distance switches trying to
12 guess the correct password in order to place free calls. Allen was charged with “accessing” the
13 telephone company computer without authorization in violation of a state computer crime statute.
14 The Kansas Supreme Court held that “access” requires gaining access “inside” the computer to
15 manipulate information and processes, and that Allen had not gone far enough. Other courts have
16 accepted broader definitions, finding that “access” refers to mere physical access to a
17 computer—for example, sending an email to a computer. See *America Online, Inc. v. National*
18 *Health Care Discount, Inc.*, 121 F. Supp. 2d 1255 (N. D. Iowa 2000) (plaintiff contended that
19 defendant had “accessed” plaintiff’s computers without authorization by harvesting email
20 addresses and sending email to plaintiff’s customers in violation of terms of service).

21 The present case, however, does not deal with such difficult facts. Nestor physically
22 interacted with the video poker machines in the manner for which they were designed. Nester
23 supplied certain information. The machines analyzed that information and produced responses.
24 The facts included in the Indictment (#12) are sufficient to show that Nestor “accessed” the video
25 poker machines.

26 II. Exceeds Authorized Access

27 Next, both Defendants argue that, even assuming the video poker machines are “protected
28 computers” and that they “accessed” the computers, their actions did not “exceed [their]

1 authorized access.” The term “exceeds authorized access” means “to access a computer with
2 authorization and to use such access to obtain or alter information in the computer that the
3 accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). The Government concedes
4 that the Defendants were authorized to play video poker. However, the Government argues that
5 the Defendants were not authorized, “ ‘to obtain or alter information’ such as previously played
6 hands of cards.” Response (#68) at 9. Essentially the Government argues that, while the
7 Defendants were allowed to play video poker, they were not allowed to play in the manner that
8 they did.

9 The majority of “exceeding authorized access” cases have to do with employees using
10 their employers’ computers. These cases generally discuss the employers’ computer use
11 restrictions which serve to inform the employee exactly what information they are allowed to
12 access on their employer’s computers. In the context of employer-employee relations, there are
13 many ways an employer traditionally limits an employee’s ability to use their employer’s
14 computers “to obtain or alter information,” e.g. terms and conditions, employment agreements,
15 job descriptions, management supervision, password protection, encryption, etc. However, most
16 of these are inapplicable in the context of the casino-patron relationship.

17 Casinos have other means of limiting their patrons’ access. For example, when playing
18 ordinary, non-video poker at a casino there is an intermediary, namely the dealer, who is
19 employed by the casino and who upholds and enforces the rules. When playing video poker, on
20 the other hand, the rules are upheld and enforced by the gambling software itself. The Defendants
21 argue that they could not have possibly exceeded their authorized access, because the bounds of
22 their authorized access were defined by what the gaming software would allow. Any selections
23 that would have exceeded that authorization should have been regulated by the software and
24 made unavailable. The software is designed to regulate what selections are allowed and what
25 results may be produced. Like the human casino employee, the software acts as the gatekeeper,
26 stopping any unauthorized access in the event that a player tries to do something that falls outside
27 the rules.

28 The Ninth Circuit’s most recent opinion interpreting the meaning of “exceeds authorized

access” makes clear that the Government’s proposed interpretation of the statute in the present case is untenable. In *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012), the government argued that “exceeds authorized access” should “refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information.” The government in *Nosal* asserted that the word “so” in the definition of “exceeds authorized access” should be read to mean “in that manner,” which it claimed referred to use restrictions. *Nosal*, 676 F.3d at 857.

Writing for the court, Chief Judge Kozinski stated that

[t]he government’s interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word that is essentially a conjunction. If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.

Id. The *Nosal* court explicitly held that “the phrase ‘exceeds authorized access’ in the CFAA does not extend to violations of use restrictions.” *Nosal*, 676 F.3d at 863. The government’s interpretation of the CFAA would “transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.” *Nosal*, 676 F.3d at 860. For example, Judge Kozinski envisioned a future where employees who are otherwise allowed to access the internet at work could be held criminally responsible under the statute for visiting ESPN.com or www.dailysudoku.com. *Id.*

Here, the Government has asserted that, although the Defendants were authorized to play the video poker machines and access information for that purpose, the way that they used the information exceeded their authorization. This argument is directly analogous to the government’s argument in *Nosal* and it fares no better here. As *Nosal* makes clear, the CFAA does not regulate the way individuals use the information which they are otherwise authorized to access. Here, the Defendants’ alleged actions did not exceed their authorized access.

III. Unconstitutionally Vague

Defendant Nestor argues that dismissal in this case is appropriate because 18 U.S.C. § 1030(a)(4) is unconstitutionally vague. Nestor Motion (#57) at 9. Because the Court finds that Defendants’ Motions to Dismiss (#56) (#57) should be granted based on other grounds, there is

no need for the Court to address Nestor's arguments concerning vagueness.

RECOMMENDATION

Based on the foregoing and good cause appearing therefore,

IT IS THE RECOMMENDATION of the undersigned Magistrate Judge that the Defendant Kane's Motion to Dismiss (#56) be **GRANTED**.


FURTHER, IT IS THE RECOMMENDATION of the undersigned Magistrate Judge that Defendant Nestor's Motion to Dismiss (#57) be **GRANTED**.

FURTHER, IT IS THE RECOMMENDATION of the undersigned Magistrate Judge that Defendant Kane's Motion for Joinder (#62) be **GRANTED**.

NOTICE

Pursuant to Local Rule IB 3-2 **any objection to this Report and Recommendation must be in writing and filed with the Clerk of the Court within fourteen (14) days after service of this Notice.** The Supreme Court has held that the courts of appeal may determine that an appeal has been waived due to the failure to file objections within the specified time. *Thomas v. Arn*, 474 U.S. 140, 142 (1985). This circuit has also held that (1) failure to file objections within the specified time and (2) failure to properly address and brief the objectionable issues waives the right to appeal the District Court's order and/or appeal factual issues from the order of the District Court. *Martinez v. Ylst*, 951 F.2d 1153, 1157 (9th Cir. 1991); *Britt v. Simi Valley United Sch. Dist.*, 708 F.2d 452, 454 (9th Cir. 1983).

DATED this 15th day of October, 2012.


ROBERT J. JOHNSTON
United States Magistrate Judge